Ohio Attorney General's

# Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

**Consumer Advocate**
**February 2020**

## Answer Only the Real Government Census, Not Scams

Every 10 years, the U.S. government counts each person living in the country. By April 1 of this year, every home across the nation will have received an invitation from the U.S. Census Bureau to participate in the 2020 census. With this in mind, it is important to understand what to expect and to be on the lookout for potential scams attempting to steal money or personal information.

In March, the U.S. Census Bureau will send invitations *via the postal mail* to households across the country requiring participation in the national census. Once you have received an invitation, you are required to respond either online, by phone or by mail. This is the first year people will have the option to respond to the census online.

In May, the U.S. Census Bureau will start following up in person with non-responsive households. The census employees will attempt to conduct the census up to six times, each time leaving a door hanger with information about who to call to schedule a visit.

The U.S. Census Bureau's official website for the census, 2020census.gov, highlights ways to avoid possible scams or frauds that try to exploit the census. To protect yourself from potential online or phone scams, be aware that the U.S. Census Bureau will never ask for:

- Your full Social Security number;
- Your bank account, credit card numbers or passwords;
- Money or donations;
- Anything dealing with political parties.

Click here to view all of the questions asked in the 2020 census. The personal information you furnish is kept confidential under federal law and is only used for statistical purposes.

If someone visits your home to collect a response for the 2020 census, it will only be because your home has not yet responded by phone or online. There are steps you can take to verify the person's identity. The individual:

- Must present a valid ID badge that includes their photograph, a U.S. Department of Commerce watermark and an expiration date;
- May carry a Census Bureau phone, laptop and/or a bag with a Census Bureau logo;
- If asked, must provide you with supervisor contact information and/or regional office phone number for verification; and
- If asked, must provide you with a letter from the Director of the Census Bureau on the U.S. Census Bureau letterhead.

If you are visited by a census worker at home, know that they are trained to conduct the census without needing to actually go inside your home.

Someone from the U.S, Census Bureau may call you for follow-up purposes or to clarify a response. Click here for information on how to verify the call you have received is legitimate. As is the case with all phone calls, do not rely on caller ID since many scammers use spoofing technology, which allows them to put any phone number on your caller ID display.

If you suspect fraud or have specific questions about the census, call 800-923-8282 and ask to speak to a local representative from the U.S. Census Bureau.

If it is determined that the visitor who came to your door does not work for the Census Bureau, contact your local police department.

In addition to the 10-year census, the U.S. Census Bureau conducts the American Community Survey (ACS), throughout each year, sending surveys to a random sample of addresses in every state. This survey is conducted primarily online, but non-respondents are mailed a paper copy to complete about two weeks after the email is sent. Phone calls and in-person interviews are also ways to conduct the survey for those who do not complete the online ACS. To verify the legitimacy of an ACS, Ohioans can contact the Census Bureau through its Philadelphia Regional Office at 800-262-4236 from 7:30 a.m. until 5 p.m.

## Apple Customers be on Alert: iCloud and AppleCare Scam Calls Making Their Rounds

Consumers throughout the country have been getting phone calls or emails claiming to be from "Apple Support." These calls or emails allege that your iCloud account or Apple ID have been compromised. You

may be prompted to push a number to speak to Apple Support, told to call a toll-free phone number or asked to click on a link. Follow these tips to ensure you're not putting your accounts at risk.

- Don't trust your caller ID. Scammers use spoofing technology to put whatever phone number they choose on your caller ID screen. You may even see the trusted Apple logo on your phone when they call. When in doubt, hang up and contact the company using contact information you know to be legitimate. This will help you verify whether the request is part of a common scam.

- If you receive a robocall, do not push a number to speak to Apple Support or otherwise engage with the scammer. If you get a voicemail claiming your iCloud account has been hacked, do not call the phone number provided by the caller. These calls will likely be routed to a scam call center.

- Do not provide any personal identifying information to a caller, including your Apple ID, your passwords, any temporary verification codes or credit card numbers.

- Do not allow remote access to a stranger. Some scammers will ask you to allow them to remotely connect to your device to "fix a problem." If you don't know who you're talking to, they could be trying to put malicious software on your device, or charge you to fix problems that don't exist.

- Never click on links or download attachments appearing in emails when you don't know the true sender, as they may be malicious.

- If you receive an email purportedly from Apple, check the grammar carefully. Poor grammar is often a sign of a scam email. Also, hover your cursor over the sender's email address. Even if the name appears to be Apple Support, hovering your mouse over that name will allow you to see the real sender's email address.

- Apple offers tips and support in case you receive bogus emails, phone calls, pop-ups or other communication from scammers. Take advantage of official Apple communications for help.

- Try to search the web for help. Use search terms that describe your situation, such as "iCloud support," along with the words "scam" or "complaint." Your search will likely bring up articles and blogs to help you check whether the phone call or message you received is a scam.

These tips can be applied to any sort of imposter or phishing scam where a business contacts you out of the blue. They often express an urgency to act, which may cause some consumers to let their guard down.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

## Ohioans Alerted to Fake Third-Party License Services

Buying a license issued by a state or county should be a safe and easy process, but recent reports allege that third-party websites are posing as official sites, taking money and failing to deliver licenses. What's more, some of these third-party sites are listed at the top of search engine results because companies can pay to be listed first. These websites look very official, but consumers who take a closer look will find that these sites are not affiliated with the government at all.

Recently, the Ohio Attorney General's Office received complaints against ohiofishinglicense.online, where people were led to believe they could obtain a fishing license. However, the official site for obtaining a fishing license in Ohio is Wildlife.OhioDNR.gov. Consumers report after clicking on the third-party website and paying to receive a fishing license, no license was ever received.

The Franklin County Auditor, who issues official dog licenses in central Ohio, recently warned about another suspicious website, ohdoglicense.com, selling fake licenses; the official site is DogLicense.FranklinCountyOhio.gov.

At best, these types of websites are bad deals for consumers, who stand to pay inflated prices for the same services they could obtain from the legitimate government office. At worst, consumers may be tricked into applying for licenses through imposter websites, submitting money and personal information, and getting a phony license or nothing in return.

After submitting sensitive information – such as their driver's license, Social Security and credit card numbers – the third-party companies have the information they need to commit identity theft or resell that information for criminal purposes.

Be sure to follow these tips:

- Most official government websites have an internet address that ends in ".gov" or ".us."
- Understand that many popular search engines accept payment to place search results at the top of the page; this allows private companies to get their product or service among the top search results when consumers enter certain keywords. Those results are typically marked as "sponsored" or "ad." Scrolling past these results will likely lead to the legitimate license application and information from the proper government agency.
- Find out what government entity regulates the license you seek. Call the legitimate phone number or go to the official website for that agency to find out how to apply for the license.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

## Tax Filers: Beware of Scams and "Ghost" Tax Preparers

As millions of Americans gather their paperwork and prepare to file their taxes, consumers should use extra vigilance as scammers continue to steal identities and money.

Recently, the Internal Revenue Service (IRS) issued a warning to avoid "ghost" tax preparers. Under the law, those who are paid to prepare federal returns must sign the return and include their valid Preparer Tax Identification Number (PTIN). However, ghost tax preparers are unethical and refuse to sign their clients' tax forms, instead instructing them to sign it and mail it on their own.

According to the IRS, ghost tax preparers may also "require payment in cash only and not provide a receipt; invent income to qualify their clients for tax credits; claim fake deductions to boost the size of a refund; or direct funds into their bank account, not the taxpayer's account." They may simply want to make some quick cash by promising you a big refund or charging fees based on how much money you get back from the IRS.

To avoid ghost tax preparers, consumers should always check a tax preparer's credentials before giving out any personal records or information. For example, review information in the IRS' directory of federal tax return preparers, and consider asking trusted friends and family for referrals. Further, consumers using a tax preparer should never allow that preparer to submit unsigned federal returns and should not submit an unsigned tax return lacking a PTIN themselves.

Other common tax scams targeting individuals and businesses include:

- **IRS impostor scams**: This scam generally begins with a phone call claiming you owe back taxes, a penalty or that a warrant has been issued for your arrest. You're told to call a certain number immediately, and eventually, you're asked to send money or to provide personal information to resolve the supposed problem.
- **Tax identity theft**: Tax identity theft generally occurs when someone steals your personal information to file a tax return and fraudulently obtain your refund.
- **Business email compromise scam**: Ohioans working in human resources, personnel and payroll positions should be aware of W-2 phishing scams. Typically, a human resources or payroll employee receives an email that appears to come from the boss or the head of the organization. The email instructs the employee to send the W-2s of all employees. Although the email may appear legitimate, it's actually part of a phishing scam attempting to expose employees' personal information.

Tips to avoid tax scams include:

- **File your tax return promptly:** This makes it less likely that an impostor will be able to file a tax return in your name to steal your refund.
- **Don't respond to threatening calls**: If you receive an unexpected phone call from someone who threatens to arrest you for not paying taxes, it's probably a scam. Don't respond to the call, and don't provide payment or personal information over the phone.

- **Don’t pay taxes using gift cards**: Con artists often ask people to buy gift cards and then read the card numbers over the phone. Using this information, they can drain funds from the card, making it difficult to trace or recover the money. The real IRS won’t demand that you pay over the phone or by using a gift card.
- **Protect your personal information**: If you file your taxes online, make sure you use a secure internet connection. If you file by mail, take your completed return directly to the post office. Keep sensitive documents in a secure place. Before getting rid of any unneeded documents that contain your Social Security number or other sensitive information, shred them.
- **Watch out for phishing scams**: Be wary of email messages that appear to come from your boss, your financial advisor or your bank, asking you to provide personal information. The message may be part of a phishing scam.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General’s Office at www.OhioProtects.org or 800-282-0515.